Hogeschool van Amsterdam

Dataprotocol

Kenniscentrum Bewegen, Sport en Voeding

Auteur: Niek van Ulzen
Datum: 07-10-2016
Versie: 0.3

Vastgesteld door het FBSV kern-LEDI op 30-09-2016.

Versiebeheer

Nummer	Datum	Opgesteld door	Omschrijving/Wijzigingen
0.1	20-08-2016	Niek van Ulzen	Initiële versie
0.2	06-09-2016	Niek van Ulzen	Opmerkingen Janine Stubbe, Sander Bliekendaal, Janey van Asperen, Mariette van Selm en Jan Botman verwerkt
0.3	07-10-2016	Niek van Ulzen	Vastgesteld op 30-09-2016 door het kern-LEDI

Gerelateerde documenten

Naam	Locatie
Gedragscode voor gebruik van persoonsgegevens in wetenschappelijk onderzoek	V:\DBSV\Projecten\Projecten\Kenniscentrum BSV\Datamanagement\Gerelateerde_Documenten
HBO Gedragscode praktijkgericht onderzoek	Idem
HvA RDM-beleid	Idem
HvA RDM-richtlijnen	Idem
HvA regeling Intellectueel eigendom	Idem
KC BSV DMP-template	V:\DBSV\Projecten\Projecten\Kenniscentrum BSV\Datamanagement\ \KCBSV_DataManagementPlan
Protocol FBSV-archief	V:\DBSV\Projecten\Projecten\Kenniscentrum BSV\Datamanagement\FBSV_Archief

Tot stand gekomen in samenwerking met

Naam	Functie
Janey van Asperen	Beleidsmedewerker onderwijs en kwaliteit FBSV, portefeuille Kwaliteitszorg
Erica Beerman	Informatiemanager ICT
Sander Bliekendaal	Manager onderzoek FBSV, portefeuille Kwaliteitszorg
Jan Botman	Informatiespecialist FBSV HvA-bibliotheek
Lea den Broeder	Lector Omgeving en Gezondheid, portefeuille Kwaliteitszorg
Aafke Hofland	Onderzoeker lectoraat Omgeving en Gezondheid
Tim van Kernebeek	Onderzoeker lectoraat Bewegingswetenschappen
Angelo Richardson	Onderzoeker lectoraat Sportzorg
Mariëtte van Selm	Projectmanager RDM-support UvA/HvA
Martinet Streppel	Onderzoeker lectoraat Gewichtsmanagement
Janine Stubbe	Lector Sportzorg, portefeuille Kwaliteitszorg
Niek van Ulzen	Datamanager, portefeuille Kwaliteitszorg

Contents

1. Afkortingen 4
2. Algemeen 5
2.1 Kenniscentrum 5
2.2 Gedragscodes 6
2.3 Intellectueel eigendom 6
2.4 Verantwoordelijkheid 7
2.5 Privacy 7
3. Planning 8
3.1 Kosten 8
3.2 Opstarten project 9
3.3 Data Management Plan 9
3.4 Toetsing door ethische commissie 10
4. Tijdens het onderzoek 11
4.1 Documentatie 11
4.2 Opslag & Beveiliging 12
5. Na het onderzoek 13
5.1 Afronding project 13
5.2 Digitale archivering en openstellen van data 13
5.3 Niet-digitale archivering 14
6. Geraadpleegde bronnen 14

1. AFKORTINGEN

Afkorting	Betekenis
CvB	College van Bestuur
CRF	Case Report Form
DIV	Documentaire Informatie Voorziening UvA/HvA
DMP	Data Management Plan
DOI	Digital Object Identifier; een permanente verwijzing (persisent identifier) en uniek label naar een digitaal object die onafhankelijk is van de bewaarlocatie. Een DOI voor een dataset is vergelijkbaar met wat een ISBN-nummer is voor een boek.
LEDI	Lectoren-en-Directie overleg KC BSV
METc	Medisch Ethische Toetsings commissie
RDM	Research Data Management
SOP	Standard Operating Procedure
WMO	Wet Medisch-wetenschappelijk Onderzoek

2. ALGEMEEN

In alle fasen van datagebruik – van het creëren/verzamelen van data tot en met het archiveren en eventueel openstellen van data – spelen ethische en juridische aspecten, privacy, data-integriteit, -opslag en -beveiliging, datalekken en toegang tot data een rol. In april 2015 heeft het CvB centrale richtlijnen vastgesteld voor research data management (RDM), de systematische en verantwoorde omgang met onderzoeksgegevens, bij de UvA en HvA. Het dataprotocol is de weerslag van de lokale uitwerking voor het kenniscentrum van die centrale richtlijnen. Punten die niet in het dataprotocol staan of punten waarvan afgeweken wordt in een project, kunnen worden beschreven in een Data Management Plan (DMP). Het dataprotocol is op kenniscentrumniveau; een DMP op projectniveau.

2.1 Kenniscentrum

1. Dit dataprotocol is in eerste instantie gericht op het onderzoek dat binnen de lectoraten van het kenniscentrum wordt uitgevoerd.
2. RDM heeft te maken met de kwaliteit van het onderzoek en heeft dus direct te maken met kwaliteitszorg. Een concrete, systematische manier van werken met onderzoeksgegevens draagt bij aan het verhogen of intact houden van de kwaliteit van onderzoek(soutput) en aan de impact ervan.
3. Het kenniscentrum moet zorgvuldig onderzoek bevorderen, dus ook zorgvuldig datamanagement. Zij voorzien in kaders en richtlijnen voor opslag en duurzame archivering, in benodigde training en in een betrouwbare (technische) infrastructuur, complementair aan reeds bestaande UvA/HvA data-gerelateerde diensten.
4. RDM is constant aan technologische en maatschappelijke veranderingen onderhevig. Dit dataprotocol en bijbehorende procedures dienen daarom geëvalueerd en eventueel ge-update te worden middels een jaarlijkse RDM-controlecyclus. Daarbij moet worden gelet op:
    a. Nieuwe ontwikkelingen op het gebied van RDM, privacy, beveiliging en ethiek
    b. Hoe gedragscodes en procedures in de praktijk worden nageleefd/uitpakken
    c. Hoe het staat met de capaciteit, mogelijkheden en betrouwbaarheid van de technische infrastructuur
    d. Voor welke lopende en afgesloten projecten er een DMP is
    e. Hoe onderzoekers omgaan met archivering en het openstellen van hun data
    f. Welke mensen toegang hebben tot het FBSV-archief
5. De jaarlijkse controlecyclus wordt gefaciliteerd door een datasteward. Bespreking , evaluatie en herziening vinden plaats in de portefeuille Kwaliteitszorg. De resultaten hiervan worden gepresenteerd in een LEDI. Er is een vooraf gedefinieerd tijdspad voor deze controlecyclus en eventuele herzieningen moeten geaccepteerd worden in een LEDI.
6. Het kenniscentrum stelt of wijst één of meerdere datastewards aan met een concreet takenpakket. Dit omvat in elk geval:
    a. Planning, controle en update van dit dataprotocol en bijbehorende procedures
    b. Controle van en ondersteuning bij DMPs
    c. Controle van en ondersteuning bij archiveren en openstellen van data
    d. Actie ondernemen bij datalekken
    e. Beheer sleutels en toegang voor opslag en archivering niet-digitale onderzoeksgegevens na afloop van onderzoeksprojecten
    f. Toezicht en beheer van onderzoeksgegevens in het FBSV-archief
    g. Deelname aan RDM-gremium HvA/UvA
    h. Volgen ontwikkelingen op het gebied van data management, privacy en ethiek
    i. Signaleren behoeften, wensen en/of problemen binnen onderzoeksprogramma’s

   j. Schakel tussen directie, ICTS en RDM om RDM-infrastructuur (verder) te ontwikkelen en om kennis te delen met onderzoekers
7. Middels het DMP dient niet alleen voor de onderzoeker(s) zelf maar ook voor het kenniscentrum duidelijk te zijn waar welke gegevens zijn opgeslagen.
8. Als een onderzoeker uit dienst gaat worden alle onderzoeksgegevens overgedragen aan het kenniscentrum. Dit gebeurt in overleg met de betreffende lector en datasteward en/of manager onderzoek[1].
9. Het kenniscentrum voert een transparant beleid over RDM-gerelateerde kosten die opgenomen kunnen worden in projectbegrotingen.
10. Het kenniscentrum heeft een heldere procedure met betrekking tot datalekken.
11. Het kenniscentrum helpt mee aan het opstellen van concrete regels over hoe onderzoekers data van topsporters of sportbonden kunnen en mogen gebruiken zonder daarbij de belangen van die topsporters en sportbonden uit het oog te verliezen (denk aan intellectueel eigendom, privacy, informed consents, concurrentie).

2.2 Gedragscodes

1. Onderzoekers en studenten dienen ten minste op de hoogte te zijn van en te handelen naar:
   a. HBO gedragscode praktijkgericht onderzoek
   b. Gedragscode voor gebruik van persoonsgegevens in wetenschappelijk onderzoek[2]
2. Een lector maakt onderzoekers, studenten en medewerkers in zijn/haar kenniskring of lectoraat attent op bovenstaande gedragscodes.
3. Bij de jaarlijkse RDM-controlecyclus wordt geëvalueerd of en hoe deze gedragscodes in de (onderzoeks)praktijk worden toegepast.

2.3 Intellectueel eigendom

Van wie zijn de data? Wie is de producent van de databank[3]? Mogelijkheden: van de onderzoeker, de student, de faculteit, een externe partij, de financier, de sportbond, de deelnemer, etc

1. Uitgangspunt voor afspraken rondom intellectueel eigendom is de HvA Regeling Intellectueel Eigendom. Tenzij elders schriftelijk is vastgelegd (bijvoorbeeld in een overeenkomst) hoe met intellectueel eigendom om te gaan, gelden de bepalingen in deze regeling. De regeling houdt kort gezegd in:
   a. De HvA is eigenaar van tijdens een project verzamelde data; niet de onderzoeker(s) zelf
   b. Bij studenten ligt het net iets complexer en hangt het af van of het primair onderwijs of onderzoek betreft. Raadpleeg hiervoor de regeling
   c. Data zijn niet van proefpersonen maar ze hebben wel zeggenschap over gebruik en beschikbaarstelling ervan. Zij moeten daarvoor toestemming geven middels een informed consent
2. NWO (en dus ook SIA/RAAK) en ZonMw beschouwen zichzelf ook als producent van de databank en zijn daarmee mede-eigenaar van de data (zie desbetreffende subsidiebepalingen).
3. Bij topsporters en sportbonden kunnen andere bepalingen gelden. Het dient voor elke partij duidelijk te zijn hoe de vork in de steel zit (zie 4) alvorens wordt gestart met de uitvoering van het project.

[1] Manager onderzoek is Sander Bliekendaal. Datasteward is Niek van Ulzen.
[2] De gedragscode persoonsgegevens wordt op dit moment herzien i.v.m. de nieuwe Europese privacyverordening.
[3] 'Producent van de databank' is een juridische term zoals wordt gebruikt in de Databankenwet. In die wet gaat het verder over 'originele creatie' en 'substantiële investering'.

4. Bij samenwerking in een consortium of met externe partijen moeten duidelijke afspraken worden gemaakt over o.a. intellectueel eigendom en deze afspraken moeten worden vastgelegd in een consortiumovereenkomst. Onderzoekers dienen voor de start van het project contact op te nemen met een legal counsel van IXA[4]. De lector ziet er op toe dat het voor elke partij duidelijk is hoe de vork in de steel zit alvorens wordt gestart met de uitvoering van het project.
5. Ook wanneer een overeenkomst van een andere partij getekend dient te worden is het raadzaam contact op te nemen met een legal counsel van IXA.

2.4 Verantwoordelijkheid

Wie is verantwoordelijk voor de verantwoorde omgang met onderzoeksgegevens?

1. De primaire verantwoordelijkheid ligt bij degenen die de data creëren en betrokken zijn bij de (dagelijkse) omgang met data: onderzoekers, studenten/promovendi en hun begeleiders. Een DMP geeft gestalte aan deze verantwoordelijkheid.
2. Het is de gezamenlijke verantwoordelijkheid van studenten/promovendi en hun begeleiders om het beheer en gebruik van data goed te regelen en te documenteren. Begeleiders van studenten en promovendi hebben de verantwoordelijkheid om studenten en promovendi op de hoogte te stellen van geldende gedragscodes, richtlijnen en afspraken die binnen het onderzoeksproject zijn gemaakt over data management (bijvoorbeeld in een DMP).
3. Studenten dienen zich aan deze richtlijnen en afspraken te houden bij het uitvoeren van het onderzoek.
4. De principal investigator (lector) is verantwoordelijk voor een systematische en verantwoorde omgang met onderzoeksdata binnen zijn/haar lectoraat. Hij/zij is verantwoordelijk voor gemaakte afspraken met onderzoekers, studenten en externe partijen, voor up-to-date DMPs per project en voor een ethisch juiste omgang met (gegevens van) deelnemers/proefpersonen.
5. Ook als een andere partij penvoerder is of het een uitvoerende opdracht betreft, is de lector er verantwoordelijk voor dat het databeheer zorgvuldig gebeurt.
6. De decaan is bekend met elk onderzoeksproject en is eindverantwoordelijk. De decaan is verantwoordelijk voor toezicht op de naleving van het dataprotocol.
7. Als de HvA penvoerder of opdrachtgever is, is de HvA formeel eindverantwoordelijke voor alle zaken die met dat onderzoek te maken hebben.
8. De verantwoordelijkheid voor het FBSV-archief ligt bij het hoofd onderwijsbureau. De verantwoordelijkheid voor het beheer van niet-digitale onderzoeksgegevens in dat archief ligt bij de datasteward.

2.5 Privacy

Bij dataverzameling van personen moet hun privacy gegarandeerd worden. Het recht op informationele privacy komt er kort gezegd op neer dat ieder mens zoveel mogelijk zelf invloed heeft op wie wat over hem of haar weet[5].

1. Onderzoekers implementeren de ‘Gedragscode voor gebruik van persoonsgegevens in wetenschappelijk onderzoek’, daarbij specifiek lettend op de 8 regels in bijlage 1 van die gedragscode.

[4] Op het moment van schrijven is de legal counsel van IXA voor de HvA Ahlam El Yaakoubi. Zij is juriste met expertise op het gebied van o.a. overeenkomsten en contracten.
[5] Uit: De juridische status van ruwe data; een wegwijzer voor de onderzoekspraktijk. Zie hier.

2. Er worden passende beveiligingsmaatregelen voor dataverzameling, -opslag en –archivering getroffen (zie 4.2). In het algemeen geldt: hoe gevoeliger de informatie, hoe strenger de veiligheidseisen.
3. Bij het verzamelen en opslaan van persoonsgegevens dient gebruik gemaakt te worden van Europese diensten. Privacy kan namelijk minder goed gewaarborgd worden als met een Amerikaanse partij gewerkt wordt.
4. Als persoonsgegevens door een andere partij worden verwerkt, zoals bij een cloud leverancier (server, Qualtrics, SURFdrive, Research Manager) dan is een bewerkersovereenkomst[6] wettelijk verplicht. Raadpleeg daarvoor een legal counsel van IXA.
5. Verzamel niet meer persoonsgegevens[7] dan noodzakelijk voor het onderzoek.
6. Wees terughoudend met het verzamelen van bijzondere persoonsgegevens. Onder bijzondere persoonsgegevens wordt onder andere verstaan gegevens over ras, gezondheid, godsdienst, politieke gezindheid en strafrechtelijke gegevens.
7. Direct identificerende en/of contactgegevens worden zo snel mogelijk verwijderd uit het onderzoeksbestand en opgeslagen in een apart communicatiebestand. Dit bestand is administratief gelinkt met het onderzoeksbestand en staat op een andere locatie (met andere toegangsvereisten).
8. Eenzelfde scheiding dient gemaakt te worden indien gegevens in een database worden opgeslagen.
9. Indien over langere tijd een systematische database met direct identificeerbare persoonsgegevens beheerd wordt, dient de lector of projectleider te verifiëren of de database geregistreerd dient te worden bij het College Bescherming Persoonsgegevens (via de functionaris gegevensbescherming van de HvA/UvA).
10. Een communicatiebestand dient vernietigd te worden wanneer het niet meer nodig is voor het doel van het onderzoeksproject. Zodoende blijft alleen een bestand over met anonieme of indirect identificerende persoonsgegevens.
11. Het is in de meeste gevallen wettelijk verplicht om deelnemers om toestemming te vragen (middels een informed consent) voor het verwerken van persoonsgegevens en om ze te wijzen op hun rechten en plichten. Het is raadzaam om zo'n informed consent aan een ethische commissie, jurist of privacydeskundige voor te leggen.
12. Bij het openstellen van data na afloop van een onderzoek zit je al snel met het niet kunnen waarborgen van de privacy. Anonieme of geanonimiseerde gegevens kunnen zonder problemen opengesteld worden hoewel enige voorzichtigheid geboden is bij hergebruik of het combineren van die gegevens met een ander databestand. Voor databestanden die persoonsgegevens bevatten moet nagedacht worden over openstellen. In veel gevallen zal dat laatste, het volledig openstellen van data, niet mogelijk zijn, maar gedeeltelijk openstellen wel (bijv. alleen de metadata).

3. PLANNING

3.1 Kosten

1. De kosten die met RDM gemoeid zijn kunnen in een projectbegroting worden opgenomen. Bijvoorbeeld:
    a. Toetsing door of verklaring van een (M)ETc

[6] Er zijn model-bewerkersovereenkomsten opgesteld door SURF en de HvA die als basis kunnen dienen.

[7] Zie bijbehorende documentatie voor het onderscheid tussen direct identificerende, indirect identificerende en bijzondere persoonsgegevens.

   b. Aanschaf software, hardware, opslagcapaciteit
   c. Hosting (cloud) server
   d. Kosten archiveren digitale data
   e. Open access publicaties
   f. Gebruik (nog in gebruik te nemen) UvA/HvA RDM-tool
   g. RDM-training onderzoekers
2. In de projectplanning kan met de volgende RDM-activiteiten rekening gehouden worden:
   a. Schrijven aanvraag (M)ETc
   b. Schrijven en bijstellen van een DMP
   c. RDM-training onderzoekers
   d. Anonimisering van data
   e. Archivering van data
   f. Openstellen van data

3.2 Opstarten project

Alvorens een project daadwerkelijk van start kan gaan, moeten er op projectmatig en op datagebied een aantal dingen gebeuren. Het projectmatig opstarten (en beheren en afronden) van een project gebeurt in afstemming met de betrokken lector, programma manager en project controller, en wordt in een ander document beschreven.

1. Er moet een Data Management Plan (DMP) geschreven worden (zie 3.3).
2. Er moet een besluit worden genomen over ethische toetsing (zie 3.4). In het DMP wordt beschreven waarom wel/niet voor ethische toetsing is gekozen en voor welke commissie is gekozen.
3. Indien met partners in een consortium wordt samengewerkt dan moet een consortiumovereenkomst opgesteld worden in samenspraak met een legal counsel van IXA. IXA heeft de expertise en een modelovereenkomst.
4. Indien verwerking (waaronder opslag) van persoonsgegevens uitbesteed wordt aan een andere partij (bijv. hosting van server/database bij een bedrijf) dan moet een bewerkersovereenkomst opgesteld worden in samenspraak met een legal counsel van IXA. IXA heeft de expertise en een modelovereenkomst (zie ook punt 4 van 2.5).
5. Bij contractonderzoek dient een schriftelijke offerte getekend te worden door de betrokken partijen (zie document voor het projectmatig opstarten van projecten) met ten minste een paragraaf over verantwoordelijkheid voor en eigendom van de data.

3.3 Data Management Plan

1. Een DMP is een digitaal document waarin de onderzoeker onder andere beschrijft welke data hoe worden verzameld, waar data worden opgeslagen en gedocumenteerd, welke beveiligingsmaatregelen zijn getroffen, hoe data gedurende en na afloop van het project (mogen) worden gebruikt.
2. Bij elk project waarvoor de HvA een aanzienlijk aandeel[8] heeft in de dataverwerking (verzamelen, opslag, bewerking, archivering), dient een DMP opgesteld te worden.

[8] Een 'aanzienlijk aandeel' dient nader geoperationaliseerd te worden. Als penvoerder, opdrachtnemer of hoofdverantwoordelijke voor een project dient in elk geval een DMP opgesteld te worden.

3. Sommige subsidieverstrekkers hebben hun eigen procedure en templates voor een DMP. In die gevallen dienen die templates gebruikt te worden. In alle andere gevallen dient gebruik gemaakt te worden van het KC BSV template.
4. Een deel van de vragen is wellicht al beantwoord in documenten voor de (M)ETc-aanvraag, in een Standard Operating Procedure of in dit dataprotocol. In die gevallen kan in het DMP naar de betreffende stukken verwezen worden.
5. Een DMP-template wordt ingevuld door één van de bij het project betrokken onderzoekers en goedgekeurd door de principal investigator (verantwoordelijke lector). Indien er een datasteward is aangesteld, controleert de datasteward het DMP op correctheid en volledigheid.
6. Binnen twee maanden na de start van het project moet een DMP in pdf-formaat opgestuurd worden naar researchdata-kcbsv@hva.nl met een standaard naamgeving[9].
7. Een DMP moet up-to-date gehouden worden gedurende de looptijd van het project. Gewijzigde versies worden naar bovenstaand e-mailadres gestuurd met een opgehoogd versienummer. Indien er een datasteward is aangesteld, controleert de datasteward eens per jaar of het DMP nog up-to-date is.
8. Na afloop van het project moet het DMP moet worden ge-update met tenminste informatie over welke data waar gearchiveerd worden en welke data al dan niet opengesteld worden.

3.4 Toetsing door ethische commissie

1. Er is geen wettelijke verplichting om een onderzoek ethisch te laten toetsen tenzij het onderzoek valt onder de WMO. Onderzoek dat valt onder de WMO wordt 'WMO-plichtig' genoemd. Toch is het ook voor niet WMO-plichtig onderzoek aan te bevelen om een ethische commissie[10] te raadplegen:
    a. om feedback te krijgen over de ethische aspecten van het onderzoek (wat zijn de lasten voor de deelnemers, hoe worden deelnemers geïnformeerd, op welke manier wordt er toestemming gevraagd, wat gebeurt er met de data na afronding van het onderzoek, etc) en de manier waarop privacy gewaarborgd wordt
    b. veel wetenschappelijke tijdschriften en subsidieverstrekkers vragen om een goedkeuring of verklaring van een (medisch) ethische commissie
2. Als het onderzoek WMO-plichtig is dan moet het onderzoek goedgekeurd worden door een erkende Medisch Ethische Toetsings Commissie (METc) zoals die van het VUmc of AMC.
3. Bij twijfel of het onderzoek WMO-plichtig is of omdat een verklaring nodig is dat het onderzoek niet-WMO-plichtig is, kan een METc een verklaring afgeven dat het onderzoek niet-WMO-plichtig is. Het onderzoeksvoorstel en bijbehorende documenten worden dan bekeken door het dagelijks bestuur van de METc (de hele METc-keten wordt niet doorlopen).
4. De bij punt 3 genoemde verklaring is geen ethische toetsing of goedkeuring, maar enkel een besluit of het onderzoek valt onder de WMO of niet. De aanvraag wordt inhoudelijk dus niet ethisch getoetst. De METc van het VUmc geeft als extra wel een advies.
5. Niet WMO-plichtig onderzoek kan ter toetsing langs een 'gewone' ethische commissie. Dit is met name van belang bij:
    a. Onderzoek met deelnemers die kwetsbaar zijn vanwege hun leeftijd, sociaal-economische, fysieke, mentale of emotionele status

[9] Standaard naam:
DMP_[Naam project aan elkaar]_[Achternaam PI aan elkaar]_[startdatum project in yyyymmdd]_[versienr].pdf

[10] Opgemerkt moet worden dat er op dit moment geen ethische commissie is voor praktijkgericht onderzoek. Een ethische commissie van bijvoorbeeld de Faculteit der Gedrags- en Bewegingswetenschappen (VU) kan met de juiste connecties benaderd worden, maar deze is niet altijd ingericht om praktijkgericht onderzoek te kunnen beoordelen.

   b. Verwerking van bijzondere persoonsgegevens
   c. Online onderzoek waarbij persoonsgegevens worden verwerkt
6. Bij onderzoek met mensen moet een informed consent verkregen worden alvorens het onderzoek wordt uitgevoerd.
7. Probeer bij een informed consent rekening te houden met de mogelijkheid dat data (deels) worden opengesteld en (dus) gebruikt kunnen worden voor onderzoek met een ander doel dan waarvoor proefpersonen meedoen (maar zie punt 10 van 2.5). Denk in elk geval al na over eventueel toekomstig hergebruik van data en hoe dat juridisch/ethisch goed af te dekken.
8. Voor gebruik van video/audiomateriaal en verwerking van bijzondere persoonsgegevens moet expliciet toestemming gevraagd worden.

4. TIJDENS HET ONDERZOEK

4.1 Documentatie

1. Data moeten op zo'n manier worden opgeslagen, gedocumenteerd en georganiseerd dat op eenvoudige wijze:
   a. Die data begrepen en (her)gebruikt kunnen worden
   b. Is na te gaan hoe bepaalde resultaten tot stand zijn gekomen
2. In het algemeen moeten alle tijdens het project gemaakte documenten bewaard worden, maar met name:
   a. De subsidieaanvraag (projectbeschrijving) en –toekenning
   b. De meest recente versie van het DMP
   c. De formulieren en aanvraag voor de (M)ETc plus de goedkeuring/verklaring van die (M)ETc
   d. Een brief met de toekenning van het project door de financier
   e. Een brief met de toestemming van het CvB van de HvA
   f. Gesloten en getekende overeenkomsten / offertes
   g. Getekende informed consent formulieren
3. Beschrijving van de gebruikte meetprotocollen/ hardware/ software/ samping rate/ etc voor dataverzameling. Die beschrijving kan in het DMP of in het DMP wordt verwezen naar de betreffende informatie.
4. Opslag van ruwe data met systematische bestandsnamen en documentatie van namen, labels, beschrijvingen van variabelen alsmede codes (en redenen) voor missing values.
5. Opslag van scripts, parameters en/of (pre)processed data en documentatie van die scripts en parameters; documentatie m.b.t. data-validatie, -checking, -cleaning, -processing en/of andere procedures m.b.t. datakwaliteit.
6. Systematisch versiebeheer.
7. Sla zoveel mogelijk op in bestandsformaten die geschikt zijn voor lange termijn opslag en toegankelijkheid. Dat wil zeggen: zo min mogelijk in een formaat dat afhankelijk is van specifieke software. DANS EASY heeft een lijst met preferred en acceptable file formats. Indien deze formats niet gebruikt kunnen worden, beschrijf dan welke software (en welke versie ervan) nodig is om het bestand te kunnen openen.
8. Software en code die ontwikkeld zijn gedurende het project moeten een duidelijk versiebeheer kennen en van voldoende commentaar zijn voorzien zodat het voor iemands anders ook mogelijk is om resultaten/figuren te kunnen repliceren.
9. Gegevens en documenten worden opgeslagen middels makkelijk herkenbare bestands- en foldernamen en systematische folderstructuur.

10. In het DMP dient nader gespecificeerd te worden welke opslagmedia worden gebruikt (i.e., waar welke data staan).

4.2 Opslag & Beveiliging

1. Onderzoekers en studenten dienen zich ten minste te houden aan de HvA ICT-gedragsregels en de door RDM-support voorgestelde maatregelen.
2. Onderzoekers nemen gepaste beveiligingsmaatregelen om dataverlies en datalekken te voorkomen. Gepast houdt in dit geval in: hoe gevoeliger/ vertrouwelijker de (persoons)gegevens, hoe strenger de beveiligingsmaatregelen die genomen moeten worden. In onderstaande punten worden die maatregelen nader gespecificeerd.
3. De projectleider maakt regelmatig ten minste één back-up op een fysiek andere locatie dan waar de originele gegevens staan.
4. Als datasets met persoonsgegevens of andere vertrouwelijke gegevens verstuurd moeten worden, dan gebeurt dit alleen versleuteld en via de HvA-mail, SURF Filesender (grote bestanden) of https/sftp.
5. Er wordt zo min mogelijk gebruik gemaakt van USB-sticks en externe harde schijven. Indien deze toch gebruikt worden (bijv. voor back-ups) dan moeten deze devices of de folders/bestanden die er op staan versleuteld worden.
6. In het DMP houdt de projectleider een duidelijk overzicht bij wie waar toegang toe heeft.
7. Data met persoonsgegevens worden tijdig en waar nodig op een consistente manier vernietigd. Bijvoorbeeld: als data via e-mail verplaats worden van een cloud server naar een netwerkschijf dan moet
    a. bekeken worden of de data nog op de cloud server moeten blijven staan of vernietigd moeten worden;
    b. de e-mail vernietigd worden nadat de overdracht heeft plaatsgevonden.
8. Maak gebruik van Europese servers en providers voor de opslag van vertrouwelijke (persoons)gegevens. Die gegevens mogen Europa niet verlaten.
9. Bij beveiliging van persoonsgegevens kan verder gedacht worden aan:
    a. Anonimiseren: Het zo snel mogelijk anonimiseren of aggregeren van data
    b. Coderen: Het aanleggen van een apart communicatiebestand (zie 2.5)
    c. Encryptie/hashing: Versleutelen van een bestand met persoonsgegevens of het hashen van persoonsgegevens zelf (bijv. hashen van wachtwoorden in een database)
10. Niet-digitale onderzoeksgegevens worden tijdens het onderzoek opgeslagen in een afsluitbare kast of la in het lab of de kamer van het betreffende onderzoeksprogramma. Indien er een datasteward is aangesteld, beheert de datasteward de sleutel voor die kast. Zo niet, dan worden er per project of onderzoeksprogramma schriftelijke afspraken vastgelegd (bijv. in het DMP).
11. Getekende informed consent formulieren moeten apart van bijbehorende onderzoeksgegevens worden opgeslagen.
12. Laat studenten met anonieme gegevens werken of met een databestand zonder direct identificeerbare gegevens. Maak hen er op attent dat ook zij vertrouwelijk met de gegevens om moeten gaan. De projectleider ziet er op toe dat de gegevens van de computer van de student verwijderd worden zodra ze hun taak hebben afgerond.
13. Bij een datalek moet de datasteward of manager onderzoek op de hoogte worden gesteld.

5. NA HET ONDERZOEK

5.1 Afronding project

1. Bij het verstrijken van de einddatum van het project moet het project afgerond worden en zal er nagedacht moeten worden hoe en welke data gearchiveerd gaan worden. Ook als dataverzameling en/of –analyses doorlopen in een ander project.
2. Binnen 6 maanden na de einddatum van het project moeten data – gekoppeld aan één of meer onderzoeksresultaten (in de vorm van bijvoorbeeld een projectrapportage, product of artikel) – gearchiveerd zijn.
3. Gegevens moeten tot ten minste 10 jaar na productie van bijbehorende onderzoeksresultaten gearchiveerd worden, tenzij eisen van de financier, wetgeving en/of afspraken die zijn gemaakt met betrokkenen een andere termijn voorschrijven.
4. Archivering is geen doel op zichzelf. Het gaat er om dat onderzoeksresultaten inzichtelijk gemaakt en verantwoord kunnen worden, ook na afloop van een project.
5. Het DMP moet worden ge-update met tenminste informatie over waar de data gearchiveerd worden en welke data al dan niet opengesteld worden.
6. De projectleider bepaalt samen met de lector en datasteward:
    a. welke data (waar) gearchiveerd moeten worden en welke vernietigd
    b. de noodzakelijke documenten die gearchiveerd moeten worden
    c. of de organisatie en (meta)documentatie op orde is
    d. welke file formats voor archivering gebruikt worden (zie)
    e. of en welke persoonsgegevens (communicatiebestand) vernietigd kunnen worden
    f. naar onderstaande punten 5.2 en 5.3

5.2 Digitale archivering en openstellen van data

1. Voor het archiveren en eventueel openstellen van data wordt vanaf 2017 gebruik gemaakt van één van de volgende geschikte[11] data repository's:
    a. Een internationale data repository
    b. Een nationale data repository zoals 4TU.ResearchData of DANS EASY
    c. Het UvA/HvA RDM-systeem
2. Gepubliceerde datasets moeten een 'persistent identifier' (bijv. DOI) krijgen. Bij bovengenoemde repository's bestaat de mogelijkheid om zo'n 'persistent identifier' toe te kennen.
3. Het kenniscentrum stimuleert het delen van data met de wetenschappelijke gemeenschap (openstellen) op basis van het principe dat data zo 'open mogelijk' moeten worden gedeeld, daarbij lettend op ethische en vertrouwelijke beperkingen. In volgorde van openheid:
    a. Onderzoeksdata en metadata zijn bij het deponeren meteen open
    b. Metadata zijn bij het deponeren meteen open; onderzoeksdata worden open na een embargoperiode
    c. Metadata zijn bij het deponeren meteen open; onderzoeksdata zijn alleen op aanvraag beschikbaar
    d. Zowel metadata als onderzoeksdata zijn niet open en alleen op aanvraag beschikbaar
4. Data worden bij voorkeur met een geschikte licentie gepubliceerd. Welke licentie en wat geschikt is, dient met de datasteward en RDM-support bepaald te worden[12].
5. Punten 1 tot en met 4 gelden ook voor data die zijn gepubliceerd bij een artikel.

[11] Voor meer informatie over wat 'geschikte' data repositories zijn: zie art. 14 van de UvA-HvA richtlijnen voor RDM.
[12] Als 'open data' de norm is dan: CC0, CC BY, CC BY-SA plus corresponderende licenties voor code/software.

5.3 Niet-digitale archivering

1. Voor de lange termijn archivering van niet-digitale onderzoeksgegevens zoals informed consents, vragenlijsten en CRFs wordt het FBSV-archief gebruikt. Deze gegevens worden dus verplaatst van de kamer/ het lab (opslag tijdens onderzoek) naar het FBSV-archief (opslag na onderzoek).
2. Voor het FBSV-archief is een apart protocol opgesteld voor het archiveren van data, de toegang tot data en de vernietiging van data (zie Protocol FBSV-archief).
3. Het FBSV-archief wordt voor zowel onderzoeks- als onderwijsgegevens gebruikt. Toegang tot het FBSV-archief verloopt via de medewerkerspas. In het FBSV-archief staan een aantal afsluitbare kasten voor onderzoekgegevens waarvan de sleutels in beheer zijn van een datasteward.
4. Het aantal personen met toegang tot het FBSV-archief wordt:
    a. Tot een minimum beperkt
    b. Inzichtelijk gemaakt
    c. Eens per jaar gecontroleerd en zo nodig bijgewerkt/opgeschoond
5. Toegang, beheer en vernietiging (na de opgegeven periode) van niet-digitale onderzoeksgegevens verloopt via een datasteward.
6. Het FBSV-archief voldoet aan de voorschriften van de dienst Documentaire Informatie Voorziening van de UvA/HvA voor de duurzame opslag van niet-digitaal materiaal (beveiliging tegen brand, diefstal, wateroverlast en andere calamiteiten). Degene die verantwoordelijk is voor het FBSV-archief ziet hier op toe.

6. GERAADPLEEGDE BRONNEN

- De juridische status van ruwe data; een wegwijzer voor de onderzoekspraktijk. SURF/CIER, 2009.
- Ethiek reglement Faculteit der Gedrags- en Bewegingswetenschappen Vrije Universiteit Amsterdam. Vaste Commissie Wetenschap en Ethiek, 2015.
- FNWI Data Protocol. Faculteit der Natuurwetenschappen, Wiskunde en Informatica Universiteit van Amsterdam, 2016.
- Gedragscode praktijkgericht onderzoek voor het HBO. Advies van de Commissie Gedragscode Praktijkgericht Onderzoek in het HBO, 2010.
- Gedragscode voor gebruik van persoonsgegevens in wetenschappelijk onderzoek. VSNU, 2005.
- Guidelines for the management of Research Data and Records. School of Economics and Management Hogeschool van Amsterdam, 2016.
- Handreiking dataprotocol. RDM-support UvA-HvA, 2015.
- Policy note quality care. MOVE Research Institute Amsterdam, 2014.
- Privacy bij wetenschappelijk onderzoek en statistiek: Kader voor gedragscode. College Bescherming Persoonsgegevens, 2002.
- Research Data Management beleid. College van Bestuur UvA-HvA, 2015.
- Vuistregel gegevensbescherming en privacy. Landelijk Coördinatiepunt Research Data Management, 2016.